BY ORDER OF THE
SECRETARYOF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 63-17

26 NOVEMBER 2001

Acquisition

TECHNOLOGY AND ACQUISITION SYSTEMS SECURITY PROGRAM PROTECTION

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: HQ USAF/XOFI (Mr Daniel Bishop) Certified by: SAF/AQX (Mr Blaise Durante)
Supersedes AFPD 31-7, 2 Mar 93 Pages: 12
Distribution: F

This policy directive implements DoD Directive 5000.1, *The Defense Acquisition System*, 23 October 2000; DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*, 10 June 2001; and DoD Directive 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*, 10 September 1997. This policy applies to all U.S. Air Force acquisition activities, including those of the Air National Guard and Air Force Reserve Component.

1. The Air Force needs quality weapons, information technology, and support systems, delivered on time, and at affordable life-cycle costs to meet mission requirements. Such systems must be inherently secure and survivable in order to operate in a hostile environment. Critical research and program technologies, systems, and information must be protected to prevent compromises that could significantly impact cost, schedule, performance, and supportability; program direction; degrade systems capabilities; shorten the life of the system; allow alteration of system capability; lead to technology transfer; or require additional resources to develop alternative countermeasures. Operational commands will evaluate, plan and program for technology and program protection requirements from mission area planning until the system is demilitarized.

2. Incidents of loss, compromise, or theft of critical program information (includes technologies and/or systems) (CPI) or critical system resources (CSR) shall be reported in accordance with DoD Instruction 5240.4 (reference (i)) and DoD 5200.1-R .

3. It is DoD policy that security is an equal partner in systems acquisition to cost, schedule, performance, and supportability. Operational commands will evaluate, plan, and program for technology and program protection requirements and supporting resources from the time mission area planning is conducted, throughout each life-cycle phase, until the system is demilitarized or approved for public release. Technical Directorate Directors (TDD) will provide for protection costs for laboratory programs until transitioned to the user or system program office.

3.1. Within the laboratory when information, technologies, and/or systems are deemed to require protection, the TDD will develop a Technology Protection Plan (TPP). Mission area planning will begin

the identification and planning cycle for critical research and program information. The TPP will transition with the technology to provide the basis for the Program Protection Plan (PPP) from Concept & Technology Development through the Systems Acquisition and Sustainment phases. The TPP will address applicable elements from para **3.2.** below. The AFRL/CC is the approval authority for TPPs. The TDD will coordinate the TPP with the operational command(s) and acquiring agency, when applicable.

3.2. Single Managers (SMs) will prepare a PPP to protect CSR and CPI. The PPP will be prepared as soon as CSR or CPI is identified, upon receipt of a TPP, Mission Need Statement (MNS), Operational Requirements Document (ORD), Program Management Directive (PMD), upon revision of a PMD, or when a System Program Office (SPO) is established. The PPP must be approved prior to Milestone B by the Milestone Decision Authority (MDA) or their designee. Approval of the PPP may not be delegated below the SM. The SM will coordinate the PPP with the operational command(s) and acquiring agency, when applicable. As a minimum, the PPP will address the following elements:

3.2.1. Technology or system description

3.2.2. Program Information

3.2.3. List of CPI to be Protected

3.2.4. List of CSR to be Protected

3.2.5. Threats to CPI

3.2.6. Threats to CSR

3.2.7. Vulnerability of CPI to the Threats

3.2.8. Vulnerability of CSR to the Threats

3.2.9. Technology Assessment/Control Plan

3.2.10. Security Classification Guides

3.2.11. System Security Engineering Considerations (Risk Mitigation)

3.2.12. Countermeasures

3.2.13. Anti-tamper Plan (To be included as a classified annex, see para **3.7.**)

3.2.14. Test Protection Planning

3.2.15. Life-cycle Protection Costs

3.2.16. Disclosure considerations as applicable to DoD Regulation 5400.7/Air Force Supplement, *DoD Freedom of Information Act Program* and DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*

3.2.17. Foreign Disclosure

3.2.18. Foreign Sales and Co-Production

3.2.19. Follow-On Support and Modification Management

3.2.20. Demilitarization

3.2.21. Command, Control, Communication, Computers, and Intelligence (C4I) Certification and Accreditation

3.2.22. Operations Security (OPSEC) Plan *[Reference AFI 10-1101)*

3.2.23. Systems Security Engineering Approach *[Reference DoD 5200.1-M]*

3.3. If no CPI or CSR are associated with a program (neither internal to the program nor inherited from a supporting program) a Technology/Program Protection Plan is not required.

3.3.1. TDDs and SMs, in coordination with SAF/AAZ, will determine the need for a TPP or PPP when special access program information is involved.

3.4. SMs will integrate protection technologies through the principles of systems security engineering (SSE). Life-cycle systems security support will identify time-phased affordable security protection alternatives and requirements, integrating them into a weapon system and supporting subsystems security architecture, other required equipment, and supporting facilities using risk management principles based on valid threat information. SMs will coordinate life-cycle physical security standards with the operational command(s) no later than entry into Milestone B, and as necessary thereafter. The SM will develop cost-effective protection alternatives and countermeasures to protect CPI and CSR at all locations as determined by the risk.

3.5. A Counterintelligence (CI) Support Plan (CISP) will be developed for each TPP and PPP. The TDD or SM will develop a CISP with their servicing Air Force Office of Special Investigation (AFOSI) Research & Technology Protection specialist. The CISP will address CI support for the life-cycle of the system or technology.

3.6. Operational commands will plan and program for protection requirements needed in all phases of the acquisition life-cycle for systems with or without a weapon system security standard, normally through the Future Year Defense Plan. Security protection requirements will be identified in needs and requirements documentation provided to the implementing, supporting, and participating commands to counter threats against CPI and CSR located at Government Owned Contractor Operated/Contractor Owned Contractor Operated (GOCO/COCO) facilities when industry protection standards do not provide the necessary physical protection.

3.7. SMs, in coordination with SAF/AQL and the supporting systems engineering function, will identify, plan, program, develop, implement, and validate anti-tamper (AT) measures, as necessary. The AT plan will be integrated and maintained as a classified annex to the PPP IAW DoD 5000.2-R. Refer to the *Anti-Tamper Security Classification Guide* for further guidance.

4. This directive establishes the following responsibilities and authorities:

4.1. The Assistant Secretary of the Air Force (Acquisition), ASAF(A), as the Air Force Acquisition Executive, is responsible for policy and resource advocacy, to include planning and programming oversight of Modernization Planning; RDT&E; Acquisition System Security; and Program Protection activities to protect critical program research and program information, technologies, and systems.

4.2. The Program Executive Officer and the Designated Acquisition Commander exercise the authority of the ASAF(A) and are responsible for ensuring implementation of appropriate system security and program protection measures by the SM or TDD for programs under their cognizance.

4.3. The Deputy Assistant Secretary (Management Policy and Program Integration), SAF/AQX, is responsible for program protection planning and programming policy.

4.4. The Assistant Secretary of the Air Force (Acquisition), Directorate of Special Programs, SAF/AQL, is responsible for AT security guidance, planning, and generic technology development.

4.5. The Administrative Assistant to the Secretary of the Air Force, Directorate of Security and Special Programs, SAF/AAZ, is responsible for special access program security management functions.

4.6. The Deputy Under Secretary of the Air Force (International Affairs), SAF/IA, is responsible for international programs and the release of information, technology, military services and weapons systems through security assistance, cooperative research and development, military exercises and training, commercial exports and other management activities with foreign nations, allies and international organizations.

4.7. The Deputy Chief of Staff/Air and Space Operations, Directorate of Security Forces, HQ USAF/XOF, provides oversight on all program protection planning policies impacting security forces areas of responsibility. HQ USAF/XOF is responsible for policy guidance on product and physical security for protection level 1-4 assets in production, deployment, maintenance, test, or undergoing modifications, as well as policy and guidance for the Information, Industrial, and Personnel Security Programs.

4.8. Headquarters Air Force Command, Control, Communications, and Computer (C4) Plans and Policy, HQ USAF/SCX, is responsible for establishing policy to ensure C4 systems are acquired, operated and maintained, and for establishing communications security (COMSEC) and computer security (COMPUSEC) policy for the protection of communications and computer systems.

4.9. The Deputy Chief of Staff/Air and Space Operations, Directorate of Intelligence, Surveillance, and Reconnaissance, HQ USAF/XOI, is responsible for establishing intelligence support policies encompassing technology targeting, threats from foreign interests, and Sensitive Compartmented Information (SCI) security management within the PPP.

4.10. The AFOSI, Counterintelligence Division, HQ AFOSI/XOQ, is responsible for ensuring life-cycle CI support through the CISP. This mission is performed using investigative tools and services from the CI, criminal, information operations, and fraud disciplines coupled with analytical assistance to identify, interpret, manage, disseminate, and neutralize threats.

4.11. Headquarters Air Force Materiel Command, Office of Security Forces, HQ AFMC/SF, provides policy advice and assistance to HQ USAF/XOF.

4.12. Operational commands are responsible for planning and programming for security manpower, equipment, and facilities requirements being designed into the systems architecture throughout RDT&E, acquisition, and sustainment phases which are in lieu of approved security systems and technologies.

5. Attachments:

5.1. See **Attachment 1** for sample compliance measurement with this policy.

5.2. See **Attachment 2** for publications that implement and interface with this policy.

JAMES G. ROCHE
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD Directive 5000.1, *The Defense Acquisition System*, 23 October 2000

DoD 5200.1-M, *Acquisition Systems Protection Program*, 16 March 1994

DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*, 10 June 2001

DoD Directive 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*, 10 September 1997

DoD Directive 5134.1, *Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L))*; 21 April 2000

DoD Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, 6 November 1984

DoD Instruction 5240.4, *Reporting Of Counterintelligence And Criminal Violations*, 22 September 1992

DoD Regulation 5400.7/Air Force Supplement, *DoD Freedom of Information Act Program*, 22 July 1999

Memorandum from the Under Secretary of Defense for Acquisition and Technology, *Guidelines for Implementation of Anti-Tamper Techniques in Weapon Systems Acquisition Programs*, 3 May 2000

Memorandum from the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Research and Technology Protection Program Plans*, 30 June 2000

Memorandum from the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Implementing Anti-Tamper (AT)*, 5 January 2001

AFI 10-601, *Mission Need and Operational Requirements Guidance and Procedures*, 13 August 1999

AFPD 14-1, *Intelligence Applications and Requirements Planning*, 1 June 1999

AFPD 31-1, *Physical Security*, 1 August 1995

AFPD 61-2, *Management of Scientific and Technical Information*, 7 April 1993

AFPD 63-1, *Acquisition System*, 31 August 1993

AFI 10-1101, *Operations Security*, 31 May 2001

AFI 33-101, *Communications and Information Management Guidance and Responsibilities*, 24 July 1998

AFI 35-101, *Public Affairs Policies and Procedures*, 1 Dec 99

Air Force Anti-Tamper Security Classification Guide, 21 May 2000

Memorandum from the Assistant Secretary of the Air Force (Acquisition), *Designation of SAF/AQL as OPR for USAF Anti-Tamper Planning*, 21 May 2000

Abbreviations and Acronyms

AFOSI—Air Force Office of Special Investigation

AFRL—Air Force Research Laboratory

ASAF(A)—Assistant Secretary of the Air Force (Acquisition)

AT—Anti-Tamper

C4—Command, Control, Communications, and Computer

CI—Counterintelligence

CISP—Counterintelligence Support Plan

COMPUSEC—Computer Security

COMSEC—Communications Security

CPI—Critical Program Information

CSR—Critical System Resource

FYDP—Future Year Defense Plan

GOCO/COCO—Government Owned Contractor Operated/Contractor Owned Contractor Operated

MDA—Milestone Decision Authority

OPSEC—Operations Security

PMD—Program Management Directive

PPP—Program Protection Plan

RDT&E—Research, Development Test, and Evaluation

SCI—Sensitive Compartmented Information

SM—Single Manager

SPD—System Program Director

SPO—System Program Office

SSE—System Security Engineering

TDD—Technical Directorate Director

TPP—Technology Protection Plan

Terms

Anti-Tamper (AT)—Anti-Tamper is defined as the systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems.

Counterintelligence Support Plan (CISP)—The CISP is a formally coordinated action plan for CI support to protect research and technology at specific DoD research, development, test, and evaluation facilities and acquisition programs. The plan addresses key aspects of the installation, the activity or program, and the nature of the CI activities to be employed. A separate plan may be prepared for each DoD contractor or academic institution where CPI or CSR are involved.

Critical Program Information (CPI)—CPI is program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat effective life of the

system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such critical programs, technologies, or systems.

Contractor Owned/Contract Operated (COCO)—An industrial facility owned and operated by a contractor.

Critical System Resources (CSR)—CSR are those resources, that if unavailable or compromised, could seriously impact development, production, delivery, or operation of a system, component, or technology. An example of a CSR would be a patented chemical compound necessary to a critical production process that is produced at a single location. In this example neither the chemical nor the process, but the single manufacturing location and their ability to produce this compound is the CSR.

Government Owned/Contractor Operated (GOCO)—An industrial facility owned by the government, but operated by a contractor.

Mission Area Assessment (MAA)—The MAA identifies mission needs using a strategy-to-task process, which links the need for military capabilities to the strategy provided by the Chairman of the Joint Chiefs of Staff (CJCS).

Mission Area Plan (MAP)—A strategic planning document covering approximately 25 years, the MAP is derived from the Mission Area Assessment and Mission Need Analysis. The MAP records the proposed plan for correcting identified mission deficiencies. It expresses non-materiel solutions, including changes in force structure, system modifications or upgrades, science and technology applications, and new acquisition programs.

Mission Needs Statement (MNS)—A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept and Technology Development Phase of Pre-Systems Acquisition.

Operational Requirements Document (ORD)—A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or the user's representative at each milestone beginning with Milestone Bsystem Development and Demonstration of the Systems Acquisition process.

Program Management Directive (PMD)—The official Air Force document used to direct acquisition responsibilities to the appropriate major commands, agencies, program executive office, or designated acquisition commander. All acquisition programs require PMDs.

Program Protection Planning—An acquisition and logistics managed program process that identifies a system's critical program elements, threats, and vulnerabilities throughout the system's life-cycle. Program Protection Planning is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes. through the integration of embedded system security processes, security manpower, equipment, and facilities.

Sensitive Compartmented Information (SCI)—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DoD 5200.1-R, *Information Security Program.*)

Single Manager (SM)—A military department of agency designated by the Secretary of Defense to be

responsible for management of specified commodities or common service activities on a Department of Defense-wide basis.

Special Access Program (SAP)—A sensitive program, approved in writing by a head of agency with original top secret authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.

System Program Office (SPO)—The office of the SM and the single point of contact with industry, government agencies, and all other life-cycle activities throughout the systems acquisition and sustainment processes.

Systems Security Engineering (SSE)—An element of system engineering that applies scientific and engineering principles to identify and reduce system susceptibility to damage, compromise, or destruction; and the identification, evaluation, and elimination or containment of system vulnerabilities to known or postulated security threats in the operational environment.

Technical Directorate Director (TDD)—The Air Force Research Laboratory (AFRL) is one laboratory made up of multiple technical directorates. Each technical directorate is led by a single “Director,” who is responsible for the technology programs that occur at their particular directorate.

Technology Protection Plan (TPP)—Similar to the PPP developed in the acquisition cycle, a TPP is developed by research organizations that identify CPI or CSR requiring increased protection.

Attachment 2

MEASURING COMPLIANCE WITH POLICY

A2.1. Compliance with planning and integrating security in the laboratory and acquisition process will be assessed in three areas: TDD policy implementation, SM policy implementation, and timeliness of PPP implementation.

A2.1.1. When information, technologies, and/or systems are deemed to require protection, the TDDs will develop a Technology Protection Plan. Compliance with this policy will be assessed by the AFRL/CC by measuring the total number of programs with CSR or CPI against the number that have prepared a Technology Protection Plan. See **Figure A2.1.**

A2.1.2. All acquisition programs must prepare a PPP, unless waived in writing by the MDA. Compliance with this policy will be assessed by the responsible MDA by measuring the total number of programs requiring a PPP against those that have prepared a PPP. See **Figure A2.2.**

A2.1.3. Early identification and protection of CPI and CSR are synonymous to cost, schedule, performance, supportability, and security. Compliance with this policy will be assessed by the responsible MDA by measuring the total number of acquisition programs with CPI and/or CSR against those with an approved PPP prior to entering Milestone B. See **Figure A2.3.**

A2.2. TDDs and SMs will consolidate the data collected and forward the previous calendar year data report to AFRL/CC and MDAs with a copy to SAF/AQX and HQ USAF/XOFI, via RCS: **HAF-XOF(AR)9226**, Acquisition Security Measurement Report by 1 February. Data will be collected effective 1 January through 31 December each year. Discontinue reporting during MINIMIZE.

Figure A2.1. Sample Metric of Laboratory Programs with CPI and/or CSR with Technology Protection Plans.

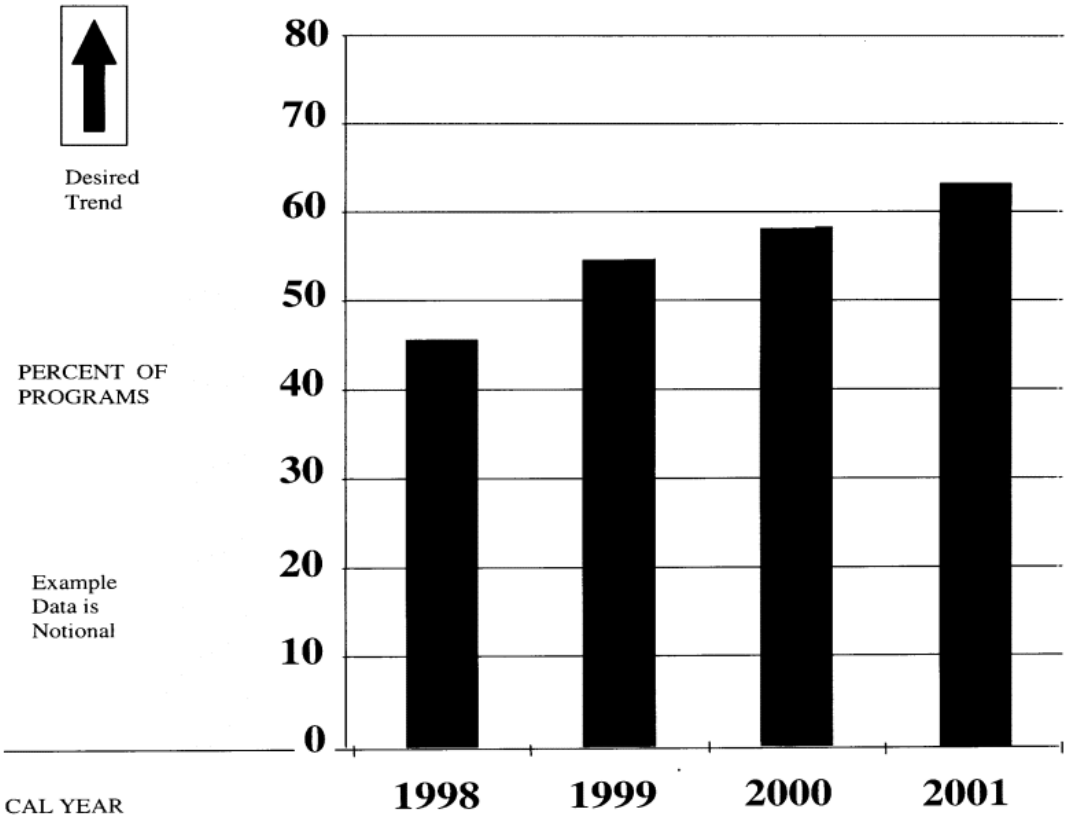

Figure A2.2. Acquisition Programs with Program Protection Plans.

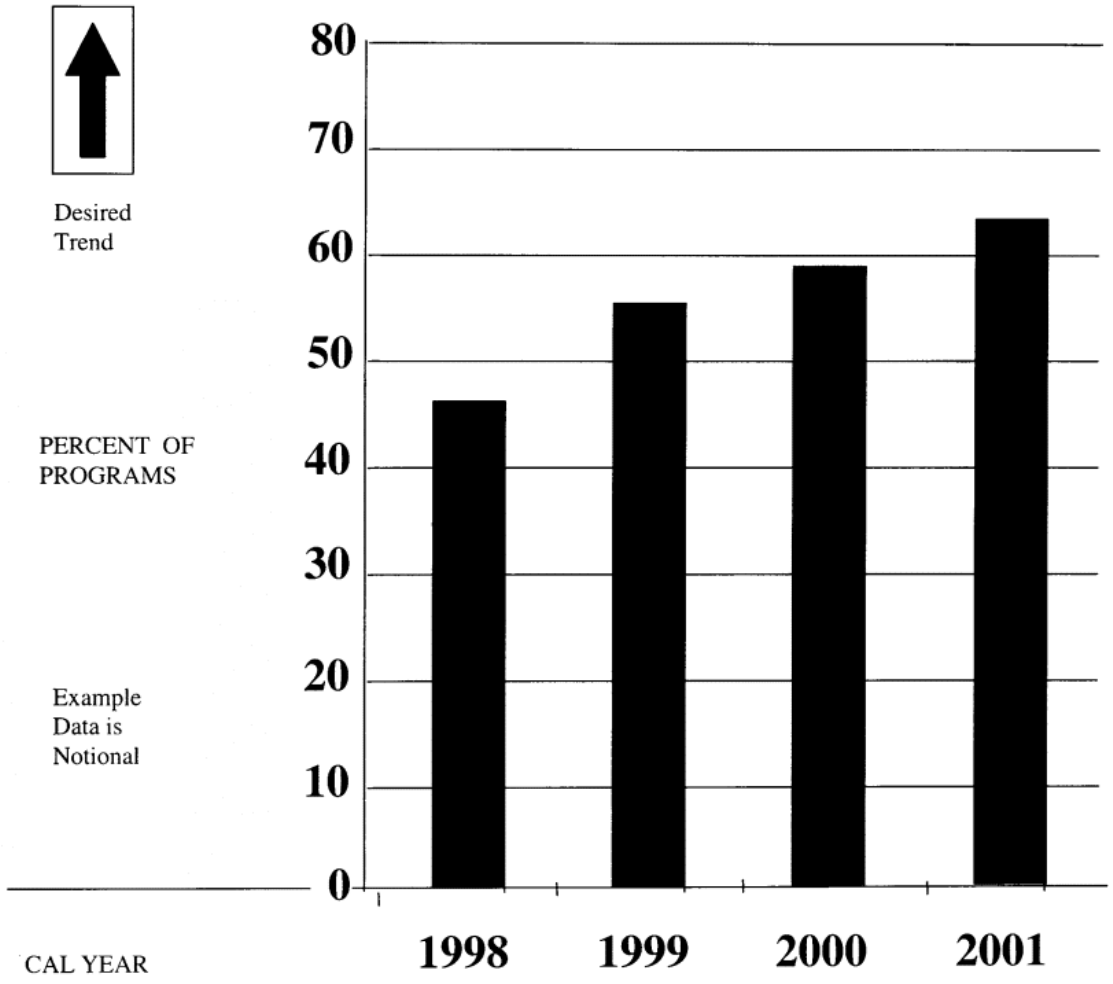

Figure A2.3. Acquisition Programs with Program Protection Plans Before Entering Milestone B.